UNITED STATES PATENT AND TRADEMARK OFFICE

4

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/859,608	05/17/2001	Pankaj B. Patel		4992

7590 12/16/2004

PANKAJ B. PATEL
1900 N. NEBRASKA AVE.
TAMPA, FL 33602

EXAMINER	
JACK, TODD M	
ART UNIT	**PAPER NUMBER**
2133	

DATE MAILED: 12/16/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/859,608	**Applicant(s)** PATEL, PANKAJ B.	
	Examiner Todd M Jack	**Art Unit** 2133	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _17 May 2001_.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-9_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-9_ is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _17 May 2001_ is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application (PTO-152)

6) ☒ Other: _Office Action_.

DETAILED ACTION

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-2, 4-6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bianco (6,256,737 B1) in view of Eberhard (5,473,689), further in view of Tatebayashi et al (6,049,611).

Claim 1: Bianco teaches a computer with an interface to authenticate over a network system (col. 12, lines 12-22), biometric identification mechanisms or devices utilize a scientific technique to identify a user based on compared measurements of unique personal characteristics (col. 7, lines 54-57), live biometric data is matched with stored biometric data (col. 8, lines 16-17), and with a successful match, the user ID is determined (col. 26, lines 34-37). Bianco does not explicitly teach sending a random number from a remote site to a local site of a user, the use of a math table to create a cryptogram, and sending the first cryptogram from the local site to the remote site for comparison with an internally generated cryptogram. Eberhard, in an analogous art, teaches generating a random number and transmitting the number to station (col. 1, lines 44-47) and transmitting the part of a first cryptogram from one station to another, then comparing the cryptogram part in the second station (col. 1, lines 50-55).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Bianco by including the sending of random number and transmitting the cryptogram, then comparing it to another cryptogram. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Eberhard, in order to allow other users at additional sites to receive cryptograms and random numbers for authentication.

The combination of Bianco in view of Eberhard does not explicitly teach sending the first cryptogram from the local site to the remote site for comparison with an internally generated cryptogram. However, Tatebayashi, in an analogous art, teaches the authentication data is a cryptogram, which was produced by encrypting a random number (col. 2, lines 43-47).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Bianco as combined with Eberhard by including the step of producing a cryptogram generated by a random number. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Tatebayashi, in order to allow uniquely and secure cryptograms to be produced.

The combination of Bianco, Eberhard, and Tatebayashi does not explicitly teach a math table in performing an encryption. It is commonly known to one reasonably skilled in the art that the encryptions may be made by the use of a math table. Therefore, the examiner takes official notice that a person reasonably skilled in the art would make use of this technique to perform the encryption.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system as combined above by including the use of a math table in the encryption. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by that which is commonly known in the art, in order to allow specific encryptions to occur and reducing CPU time.

Claim 2: Further, Bianco teaches a present invention uses encryption to protect data within a biometric system (col. 50, lines 45-47).

Claim 4: Further, Bianco (6,256,737 B1), in view of Eberhard, further in view of Tatebayashi et al (6,049,611) in claim 1, fails to teach the step of sending the first generated cryptogram to the remote site for comparison with a second cryptogram. Eberhard teaches sending the cryptogram to a mobile carrier where it is compared with a cryptogram of another random number (col. 3, lines 63-67 and col. 4, lines 1-2).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Bianco by including sending a cryptogram to a remote site and comparing it to another cryptogram. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Eberhard, in order to allow other users at remote sites to receive cryptograms for authentication purposes.

Claim 5: Further, Bianco (6,256,737 B1), in view of Eberhard, further in view of Tatebayashi et al (6,049,611) in claim 1, fails to teach a user over a network wherein the second cryptogram is generated from a site other than from the local site. Eberhard teaches the generation of a cryptogram at a stationary station, then transmitting that cryptogram to a mobile station (col. 3, lines 65-67 and col. 4, lines 1-2).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Bianco by including the generation of a cryptogram at a stationary station, then transmitting that cryptogram to a mobile station. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Eberhard, in order to allow other users at local sites to receive cryptograms for authentication purposes.

Claim 6: Further, Bianco teaches matching a biometric template, and then authentication proceeds. (col. 26, lines 34-39)

Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bianco in view of Eberhard, further in view of Tatebayashi and Veneklase.

Claim 3: Further, Bianco (6,256,737 B1) in view of Eberhard (5,473,689), further in view of Tatebayashi et al (6,049,611) and Veneklase in claim 1, fails to teach generating a first cryptogram from the random number if the first encrypted biometric parameter positively matches the second encrypted biometric parameter. Veneklase, in an analogous art, teaches if the password matches an entry of the master password list, the analyzing means generates a command (col. 5, lines 32-41) where the password may be a biometrically produced password and the command may be a cryptogram.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Bianco by including the generation of a cryptogram upon verification of a biometric parameter match. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Veneklase, in order to assure that only authorized individuals had authority to authenticate a user.

Claims 7-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bianco in view Veneklase, further in view of that which is commonly known in the art.

Claim 7: Bianco teaches a computer with an interface to authenticate over a network system (col. 12, lines 12-22), biometric identification mechanisms or devices utilize a scientific technique to identify a user based on compared measurements of unique personal characteristics (col. 7, lines 54-57), live biometric data is matched with stored biometric data (col. 8, lines 16-17), and with a successful match, the user ID is determined (col. 26, lines 34-37). Bianco teaches that with a successful match, the user

ID is determined (col. 26, lines 34-37). Bianco fails to teach generating a second random number when the first encrypted biometric parameter does not positively match the second encrypted biometric parameter and operating on the second random number with a math table to create a first cryptogram when a positive match fails to occur between the first and second biometric parameter. Veneklase teaches if the password matches an entry of the master password list, the analyzing means generates a command (col. 5, lines 32-41) where the password may be a biometrically produced password and the command may be a cryptogram.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Bianco by generating a random number and creating a cryptogram upon the obtaining of a negative result. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Veneklase, in order to assure that only authorized individuals had authority to authenticate a user.

The examiner takes official notice that it is commonly known to one reasonably skilled in the art that one can approve an action if a negative result is found, just as easily as with a positive result.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system as combined above by approving an action if a negative result is found. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by that which is commonly known in the art, in order to allow an action to be implemented as a result of a failure to authenticate to further prevent unauthorized access to occur.

Claim 8: Further, Bianco teaches with a successful match, the user ID is determined (col. 26, lines 34-37). Bianco in view Veneklase, further in view of that which is commonly known in the art in claim 7, fails to teach approving an action if a negative result is found, just as easily as with a positive result.

The examiner takes official notice that it is commonly known to one reasonably skilled in the art that one can approve an action if a negative result is found, just as easily as with a positive result. It is commonly known in the art that one can approve an action if a negative result is found, just as easily as with a positive result.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Bianco by approving an action if a negative result is found. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by that which is commonly known in the art, in order to allow an action to be implemented as a result of a failure to authenticate to further prevent unauthorized access to occur.

Claim 9: Further, Bianco in view of Veneklase, further in view of that which is commonly known in the art in claim 7 fails to teach generating a first cryptogram from the random number if the first encrypted biometric parameter positively matches the second encrypted biometric parameter. Veneklase, in an analogous art, teaches if the password matches an entry of the master password list, the analyzing means generates a command (col. 5, lines 32-41). Bianco fails to teach that a password may be a biometrically produced password and the command may be a cryptogram. It is commonly known to one reasonably skilled in the art that a biometrically produced password and the command may be encrypted.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Bianco by including the generation of a cryptogram upon verification of a biometric parameter match. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Veneklase, in order to assure that only authorized individuals had authority to authenticate a user.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Todd M Jack whose telephone number is 571-272-3823. The examiner can normally be reached on M-Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert Decady can be reached on 571-272-3819. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Todd Jack
Art Unit 2133

December 6, 2004

ALBERT DECADY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100